

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*A Black LG Smartphone cellular telephone, secured by
the Franklin County Sheriff's Office under FCSO
Evidence #1194014

Case No. 2:23-mj-322

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A (incorporated by reference)

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*18 U.S.C. §§ 2251, 2252 and
2252A

production, receipt, distribution or possession of child pornography



The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ryan Marvich, Special Agent HSI

*Printed name and title*Sworn to before me and signed in my presence.
Via FaceTimeDate: May 22, 2023City and state: Columbus, Ohio

 Elizabeth A. Preston Deavers
 United States Magistrate Judge
 

ATTACHMENT A

The property to be searched is identified as a Black LG Smartphone cellular telephone, secured by the Franklin County Sheriff's Office under FCSO Evidence #1194014. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
List of Items to be Seized

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely 18 U.S.C. §§ 2251, 2252 and 2252A – the production, distribution, receipt, and possession of child pornography including:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography or payments for child pornography or sex trafficking of minors.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse, sexual trafficking of minors, or exploitation of minors.

6. Any and all records, documents, invoices and materials, in any format or medium
(including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.
7. Any and all files, documents, records, or correspondence, in any format or medium
(including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
9. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;
12. Evidence of the utilization of peer-to-peer file sharing programs;
13. Evidence of utilization of user names or aliases, email accounts, social media accounts, and online chat programs, and usernames, passwords, and records related to such accounts;
14. Evidence of software that would allow others to control **TARGET CELLPHONE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the

- presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;
15. Evidence indicating the computer user's state of mind as it relates to the crimes under investigation;
 16. Evidence that **TARGET CELLPHONE** were attached to any other digital device or digital storage medium;
 17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from **TARGET CELLPHONE**;
 18. Passwords, encryption keys, and other access devices that may be necessary to access **TARGET CELLPHONE**;
 19. Records of or information about Internet Protocol addresses used by **TARGET CELLPHONE**;
 20. Records of or information about any Internet activity occurring on **TARGET CELLPHONE**, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
AN A BLACK LG SMARTPHONE
CELLULAR TELEPHONE, SECURED BY
THE FRANKLIN COUNTY SHERIFF'S
OFFICE UNDER SECURED UNDER FCSSO
EVIDENCE # 1194014

Case No. 2:23-mj-322

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Ryan Marvich, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property - an electronic device - which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Your Affiant is a sworn Special Agent with the United States Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). Your Affiant has been a Special Agent within DHS since the Department's creation in May 2003. Your Affiant has been assigned to the HSI Columbus office since February 2008, where your Affiant has been involved with narcotics investigations. Prior to becoming a Special Agent with HSI, your Affiant served as an Officer with the United States

Secret Service, Uniformed Division beginning in January 1998. In June 1999, your Affiant accepted a position as a Special Agent with the United States Secret Service. In May 2003, your Affiant transferred employment to become a Special Agent with the United States Customs Service (USCS). In 2003, under the creation of the Department of Homeland Security, various components, including criminal investigators/special agents, with the USCS were merged with components, including criminal investigators/special agents, from the United States Immigration and Naturalization Service (INS) and formed U.S. Immigration and Customs Enforcement (ICE). Since then, criminal investigators/special agents and all related investigative functions of ICE have been moved into Homeland Security Investigations (HSI) within ICE.

3. Your Affiant is a federal law enforcement officer who is engaged in enforcing the criminal laws, including those related to child exploitation and child pornography violations, such as the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is identified as a Black LG Smartphone cellular telephone secured by the Franklin County Sheriff's Office under secured under FCSO Evidence #1194014, hereafter being referred to as the TARGET CELLPHONE. The applied-for warrant would authorize the forensic examination of the TARGET CELLPHONE for the purpose of identifying electronically stored data particularly described in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252 and

2252A - the production, distribution, receipt, and possession of child pornography. I am requesting authority to search the entirety of the TARGET CELLPHONE, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence, fruits, and instrumentalities of the above violations.

6. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, see 18 U.S.C. § 2711(3)(A)(i).

APPLICABLE STATUTES AND DEFINITIONS

7. Title 18, United States Code, Section 2251, makes it a federal crime for any person to knowingly persuade a minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct for the purpose of transmitting a live visual depiction of such conduct. If such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any

visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

10. As it is used in 18 U.S.C. § 2251 and 18 U.S.C. §§ 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

11. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

12. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

13. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and all Attachments hereto include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

14. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”

15. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”

16. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

17. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

18. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through

² The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

19. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

20. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

BACKGROUND REGARDING THE INTERNET AND MOBILE APPLICATIONS

21. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files (“objects”) may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

22. Computers, mobile devices, and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

23. Computers, tablets, and smart/cellular phones (“digital devices”) are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a “scanner,” which is an optical device that can digitize a hard copy photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names

including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

24. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

25. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128 Gigabytes. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro-SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily

stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

26. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information,

posting information, account application information, Internet Protocol (“IP”) addresses and other information both in computer data format and in written record format.

27. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user’s true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

28. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person “deletes” a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block

of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

29. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

30. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

31. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use

whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

32. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as “apps,” are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such “apps” include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram. Kik is a free mobile application that can be downloaded on Android or iOS devices that permits users to communicate anonymously with fellow Kik users. This application allows users to create groups where like-minded individuals can chat/text other users and post videos/images which includes groups in the sexual exploitation of children. Kik allows each user to create a unique username for their individual account when registering for the app. The username is a unique identifier that is tied to the individual’s Kik account that cannot be changed or replicated in any way. The only way for a registered user to create a new username is to shut down their Kik account and set up a new one with a different username. Kik also allows each user to create a display name. The display name is what the user shows publicly to connect with other registered Kik users. The display name can be changed at any time by the person who registered for the Kik account.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

33. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code

or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

34. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

35. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices (including internal storage such as SD cards), are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2252 and 2252A and should all be seized as such.

PROBABLE CAUSE

36. On February 12, 2019, investigators with Homeland Security Investigations (HSI) and the Franklin County Sheriff's Office (FCSO) encountered Ruben Rodriguez Jr. who was found to be in possession of two kilograms of cocaine. Investigators originally located Ruben Rodriguez Jr. on February 11, 2019, while they were conducting routine surveillance at a Red Roof Inn located at 4530 West Broad Street, Columbus. At that time, investigators observed a silver Ford Fusion bearing Texas license plate KZB9897 parked in the Red Roof Inn parking lot. Upon running this license plate in law enforcement databases, investigators learned that this vehicle was registered to a Michael Rene Ponce in Buda, Texas. Investigators also learned that

Ponce was arrested in March 2008 in Austin, Texas as part of a large heroin conspiracy case involving over a dozen other co-conspirators. Ponce was subsequently convicted for violation of Title 21 USC Section 846 (conspiracy to possess with the intent to distribute heroin) and was sentenced to 57 months in federal prison. The law enforcement databases also showed no connections to Ponce and any individuals in Ohio.

37. Investigators began surveillance on the Ford Fusion on February 11, 2019, as the driver, later identified as Ruben Rodriguez Jr. and his girlfriend, Beslin Peraza, ate lunch at a Bob Evans Restaurant located at 4331 West Broad Street, Columbus, Ohio, shopped at a Walmart near Hilliard Rome Road in Columbus and then went to see a movie at a local movie theater. It was apparent to investigators that these individuals were making attempts to "kill time" which is indicative to investigators as drug activity, specifically awaiting delivery of possible drug proceeds. While Rodriguez and Peraza were inside the Walmart, FCSO Deputy Rob McKee ran his canine "Gator" around the silver Ford Fusion while it was parked in the Walmart parking lot. Gator gave a positive alert to the presence of narcotics inside the silver Ford Fusion. Eventually, Rodriguez and Peraza checked into a different hotel, the La Quinta Inn and Suites located on 5510 Trabue Road, Columbus, Ohio.

38. On February 12, 2019, investigators re-established surveillance on Rodriguez and Peraza as they traveled to 121 Stevens Avenue, Columbus, Ohio. Upon arriving, Rodriguez was observed entering this residence where he remained for approximately ten minutes. Following his departure from this residence, a deputy with FCSO conducted a traffic stop on the vehicle Rodriguez was driving. During a subsequent search of the vehicle, approximately 2.0 kilograms of cocaine and \$30,006.00 in U.S. currency were discovered. In a subsequent interview, Rodriguez stated that he was in Columbus for the purpose of overseeing the arrival of cocaine

and heroin that was being sent to individuals at 121 Stevens Avenue, Columbus, Ohio. He admitted that the cocaine in his car had been sent to these individuals at 121 Stevens Avenue approximately 1-2 weeks ago, and he came to Columbus at that time to make sure these individuals received this cocaine. After they received this cocaine, he went back to Texas. A short time later he learned that these individuals were not happy with the quality of the cocaine, so he was sent back up to Columbus. When he arrived this time in Columbus, around February 9, 2019, he was directed by his boss in Mexico to retrieve the cocaine that was already delivered and to oversee the arrival of approximately 2 kilograms of heroin that was arriving via UPS. According to Rodriguez, when he was inside the residence located at 121 Stevens Avenue, Columbus, Ohio, he stated that he saw the 2 kilograms of heroin that was sent. It was at this time the individuals at this residence paid him a partial payment of approximately \$30,000 for this heroin. This was the money seized by investigators during the traffic stop on his vehicle. Ruben Rodriguez Jr. was arrested on federal drug conspiracy charges, specifically conspiracy to distribute heroin, at that time. He has subsequently been convicted of this charge in the Southern District of Ohio. According to law enforcement databases, a Lashawn White was listed as an occupant during the time period that Rodriguez oversaw the cocaine and heroin arriving at the residence. The vehicle known by investigators as being used by Lashawn White has been observed at 121 Stevens Avenue during this time period.

39. Additionally, investigators have learned that Lashawn White was arrested by the Ohio Highway Patrol (OHP) on April 1, 2018, after a traffic stop on Livingston Avenue in Columbus, Ohio. During this traffic stop, troopers found a small amount of cocaine in the vehicle and White had a loaded handgun under his thigh while seated in the driver's seat. According to the arresting OHP trooper, when the handgun was found, White stated that if they seized his gun,

he would just get another one because he lives on Stevens Avenue. White was arrested at that time. He subsequently was released from custody pending further court hearings.

40. On September 30, 2019, investigators identified a residence in Reynoldsburg, Ohio that they believed was being used as a "stash house" for storage and distribution of narcotics that was being supplied by individuals associated with the Latin Kings street gang in Chicago, Illinois. While investigators established 24-hour surveillance on this residence from October 18, 2019, through November 4, 2019, investigators observed that no one actually resided at this residence. Investigators did observe Lashawn White frequent this residence numerous occasions while bringing boxes and bags into and out of this residence. On November 21, 2019, investigators did execute a State of Ohio search warrant on this residence and located approximately 63 empty wrappers which appeared to be wrappers for kilogram quantities of narcotics.

41. On November 14, 2019, investigators executed a State of Ohio search warrant on the residence located at 121 Stevens Avenue, Columbus, Ohio. Upon executing this search warrant, investigators located numerous individuals inside the residence. Also found and seized from inside this residence were the following items (all weights are approximate): 180 grams of suspected powdered cocaine, 33 grams of suspected crack cocaine, 15 grams of suspected heroin, 30 grams of suspected methamphetamine, 21 tablets of suspected suboxone, 10mg/325mg Oxycodone tablets, 2mg Alprazolam tablets and five firearms. These drugs were packed for individual sale, and it was apparent to investigators that this residence was being used as a selling point for numerous kinds of narcotics. Investigators found court paperwork in the name of Lashawn White in the living room of this residence at that time.

42. On November 21, 2019, at approximately 8:42am, investigators executed a State of Ohio search warrant at 669 South Kellner Drive, Columbus, Ohio. It had been determined that this was the residence of Lashawn White after he sold cocaine to a Whitehall Police Department confidential informant. Lashawn White was the only person found to be inside the residence during the execution of this search warrant. Some of the items found by investigators during this search were as follows (all narcotics have since been tested and confirmed by the Ohio BCI laboratory): 484.44 grams of a mixture of fentanyl and Tramadol, 9.46 grams of fentanyl, 18.14 grams of cocaine, 23.71 grams of a mixture of heroin and fentanyl, 3 pistols, one sawed-off shotgun, and approximately \$20,363.00 in U.S. currency.

43. Also located in the hall closet was a Black LG Smartphone. This telephone (hereafter referred to as TARGET CELLPHONE) was seized by the Whitehall Police Department as item# 19WHI-5232-PR and transferred to the Franklin County Sheriff's Department on February 22, 2023, and secured under FCSO Evidence #1194014.

44. On March 29, 2023, your Affiant received a federal search warrant (2:23-mj-214) issued out of the Southern District of Ohio allowing investigators to conduct a forensic search/exam of the TARGET CELLPHONE of evidence related to violations of Title 21 USC Section 846- conspiracy to possess wit the intent to distribute a controlled substance.

45. During the subsequent search/exam of the TARGET CELLPHONE, Forensic Computer Specialist (FCS) Phillip Hinders with the Ohio Narcotics Intelligence Center (ONIC) obtained an extraction from the TARGET CELLPHONE and discovered a video file containing what appeared to be a prepubescent male child engaging in sexual activity with a chicken. Specifically, the prepubescent male child exposes his penis and inserts it in the rear of

the chicken. This video has been seen by FCS Hinder on other devices in the past and has been confirmed to be child pornography. Upon locating evidence of child pornography on the TARGET CELLPHONE, the search of this device was paused pending the obtaining of a new search warrant specifically allowing for the search for evidence of child pornography.

46. Based upon the above information, your affiant believes that there is probable cause that TARGET CELLPHONE contains additional evidence of child pornography.

SEARCH METHODOLOGY TO BE EMPLOYED

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of TARGET CELLPHONE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, which might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

- a. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
- b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
- c. Surveying various files, directories and the individual files they contain;
- d. Opening files in order to determine their contents;

- e. Scanning storage areas;
- f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

48. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT
TO VIEW CHILD PORNOGRAPHY**

49. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved seeking/soliciting, receiving, distributing, and/or collecting child pornography:

- a. Those who seek out, exchange and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

- b. Those who seek out, trade and/or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Those who seek out, trade and/or collect child pornography sometimes maintain hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections are often maintained for several years and are kept close by. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- d. Those who seek out, trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been

known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- e. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

50. Based upon the conduct of individuals involved in seeking/soliciting, receiving, distributing, and/or collecting child pornography set forth in the above paragraphs, and the facts learned during the investigation in this case, Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of distributing, receiving, and possessing child pornography will be located in the TARGET CELLPHONE.

CONCLUSION

51. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 2252A – the production, receipt, distribution or possession of child pornography, have been committed, and evidence of those violations will be found within the contents of the TARGET CELLPHONE. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the TARGET CELLPHONE described in Attachment A, and the seizure of the items described in Attachment B.

Respectfully submitted,



Ryan Marvich
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on May 22, 2023:



Elizabeth A. Preston Deavers
United States Magistrate Judge

